Crossing the Bridge between Similar Games

Jan-David Quesel, Martin Fränzle, and Werner Damm

University of Oldenburg, Department of Computing Science, Germany

9th International Conference on
Formal Modeling and Analysis of Timed Systems (FORMATS 2011)
Phønix Hotel, Aalborg, Denmark 21-23 September 2011

Outline

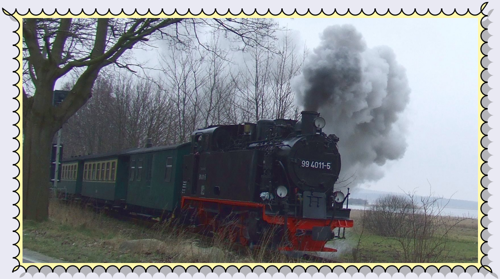
Outline

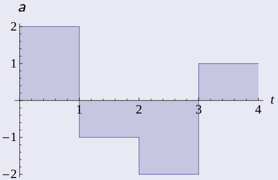
Hybrid Systems

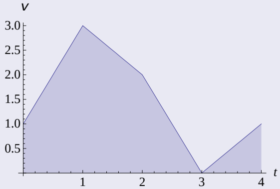
Problem

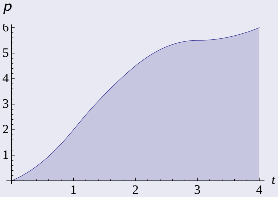
Hybrid System

- Continuous evolutions (differential equations)
- Discrete jumps (control decisions)

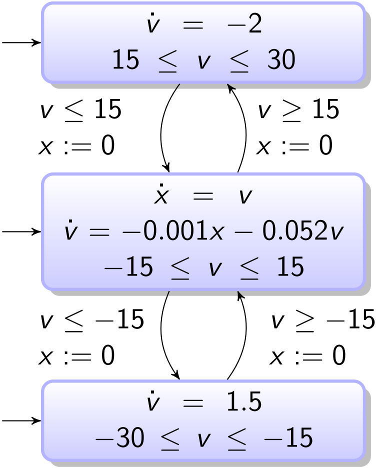


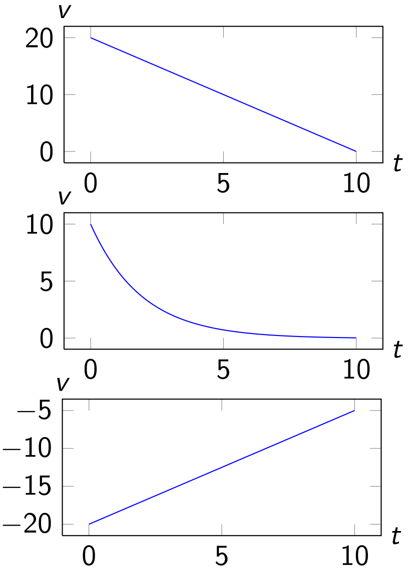




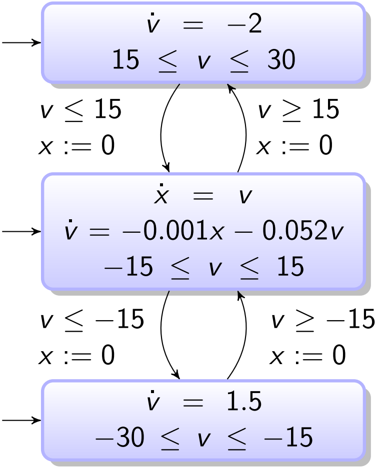


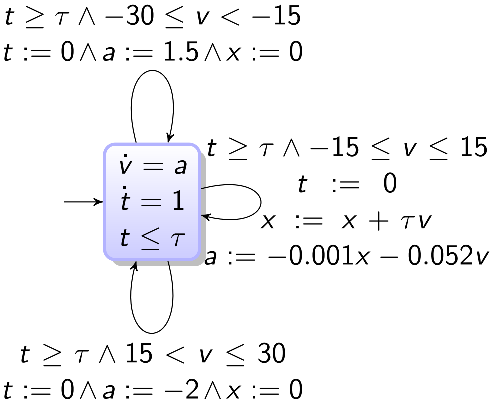
Velocity Controller



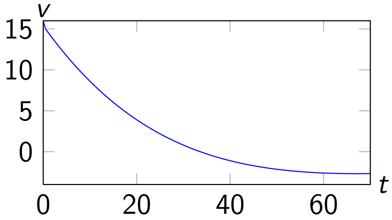


Velocity Controller

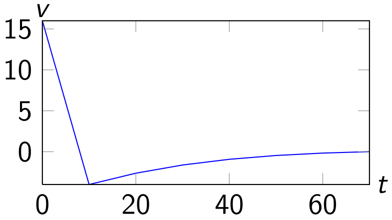




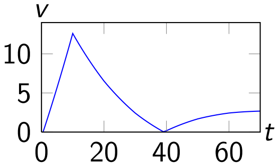
Velocity Controller



Velocity (specification)

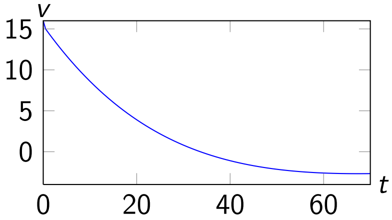


Velocity (implementation)

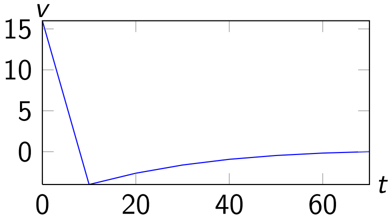


Velocity differences

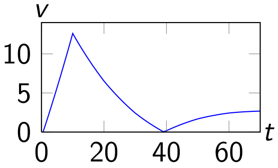
Velocity Controller



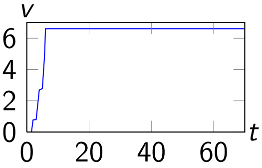
Velocity (specification)



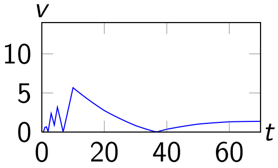
Velocity (implementation)



Velocity differences



Temporal differences



Velocity differences (retimed)

Outline

Example for the Semantics

Example

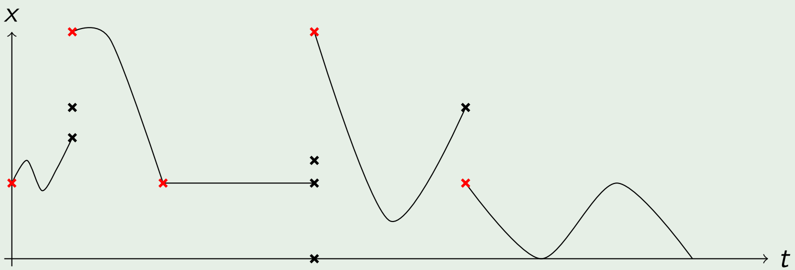
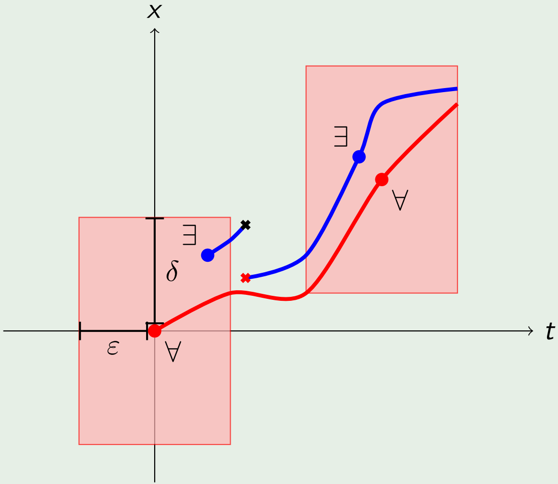


Illustration of the Similarity Notion

Example



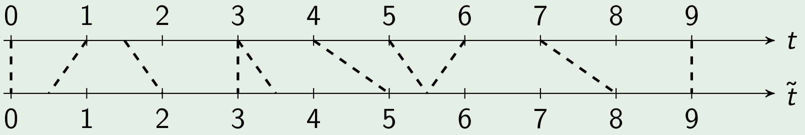
Retiming

Definition (ε-Retiming)

A left-total, surjective relation $\mathfrak{r} \subseteq \mathbb{R}^+ \times \mathbb{R}^+$ is called ε-retiming iff

$$\forall (t, \tilde{t}) \in \mathfrak{r} : |t - \tilde{t}| < \varepsilon \wedge \forall (t', \tilde{t}') \in \mathfrak{r} : (t \leq t' \to \tilde{t} \leq \tilde{t}') \ .$$

Example



Definition of ε-δ-simulation

Definition

For two streams $\sigma_i : \mathbb{R}^+ \times \mathbb{N} \to \mathbb{R}^p$ with $i \in \{1, 2\}$, given two non-negative real numbers ε, δ, we say that σ_1 is ε-δ-simulated by stream σ_2 (denoted by $\sigma_1 \trianglelefteq^{\varepsilon,\delta} \sigma_2$) iff there is a ε-retiming $\mathfrak{r}$ such that

$$\forall (t, \tilde{t}) \in \mathfrak{r} : ||c(\sigma_1)(t), c(\sigma_2)(\tilde{t})|| < \delta$$

where for $k \in \{1, 2\}$: $c(\sigma_k)$ is defined by $c(\sigma_k)(t) := \lim_{q \to \infty} \sigma_k(t, q)$.

Definition of ε-δ-simulation

Definition

A hybrid system A is ε-δ-simulated by another system B (denoted by $A \trianglelefteq^{\varepsilon,\delta} B$) iff for all input streams ι_A and for all input streams ι_B $\iota_A \trianglelefteq^{\varepsilon,\delta} \iota_B$ implies that for all output streams $\omega_A \in \Xi(\iota_A)$ of A, there is an output stream $\omega_B \in \Xi(\iota_B)$ of B such that $\omega_A \trianglelefteq^{\varepsilon,\delta} \omega_B$ holds.

Outline

Logic $\mathcal{L}\natural$ (Syntax)

Definition (Syntax of $\mathcal{L}\natural$)

The basic formulas are defined by

$$\phi ::= x \in \mathcal{I} \mid f(x_1, \ldots, x_n) \leq 0 \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \mathbb{U}_{\mathcal{J}} \phi_2$$

where $\mathcal{I} \subseteq \mathbb{R}$, $\mathcal{J} \subseteq \mathbb{R}$, f is a Lipschitz continuous function and the x_i are variables.

Logic $\mathcal{L}\natural$ (Semantics)

Definition (Valuation)

We define the valuation of a variable x at time t on a run ξ as

$$\zeta_\xi(t, x) := \lim_{n \to \infty} \xi(t, n)|_x \;\; ,$$

where $y|_x$ denotes the projection of the vector y to its component associated with the variable name x.

Logic $\mathcal{L}\natural$ (Semantics)

Definition (Semantics of $\mathcal{L}\natural$)

We define for a run ξ and some $t \in \mathbb{R}^+$ the semantics of a formula ϕ by:

- $\xi, t \models x \in \mathcal{I}$ iff $\zeta(t, x) \in \mathcal{I}$
- $\xi, t \models f(x_1, \ldots, x_n) \leq 0$ iff $f(\zeta(t, x_1), \ldots, \zeta(t, x_n)) \leq 0$

Logic $\mathcal{L}\natural$ (Semantics)

Definition (Semantics of $\mathcal{L}\natural$)

We define for a run ξ and some $t \in \mathbb{R}^+$ the semantics of a formula ϕ by:

- $\xi, t \models x \in \mathcal{I}$ iff $\zeta(t, x) \in \mathcal{I}$
- $\xi, t \models f(x_1, \ldots, x_n) \leq 0$ iff $f(\zeta(t, x_1), \ldots, \zeta(t, x_n)) \leq 0$
- $\xi, t \models \neg\phi$ iff not $\xi, t \models \phi$
- $\xi, t \models \phi \wedge \psi$ iff $\xi, t \models \phi$ and $\xi, t \models \psi$

Logic $\mathcal{L}\natural$ (Semantics)

Definition (Semantics of $\mathcal{L}\natural$)

We define for a run ξ and some $t \in \mathbb{R}^+$ the semantics of a formula ϕ by:

- $\xi, t \models x \in \mathcal{I}$ iff $\zeta(t, x) \in \mathcal{I}$
- $\xi, t \models f(x_1, \ldots, x_n) \leq 0$ iff $f(\zeta(t, x_1), \ldots, \zeta(t, x_n)) \leq 0$
- $\xi, t \models \neg\phi$ iff not $\xi, t \models \phi$
- $\xi, t \models \phi \wedge \psi$ iff $\xi, t \models \phi$ and $\xi, t \models \psi$
- $\xi, t \models \phi \mathbb{U}_{\mathcal{J}} \psi$
  iff $\exists t' \in \mathcal{J} : \xi, max\{t' + t, 0\} \models \psi$ and $\forall t \leq t'' < t' + t : \xi, t'' \models \phi$

Logic $\mathcal{L}\natural$ (Semantics)

Definition (Semantics of $\mathcal{L}\natural$)

We define for a run ξ and some $t \in \mathbb{R}^+$ the semantics of a formula ϕ by:

- $\xi, t \models x \in \mathcal{I}$ iff $\zeta(t, x) \in \mathcal{I}$
- $\xi, t \models f(x_1, \ldots, x_n) \leq 0$ iff $f(\zeta(t, x_1), \ldots, \zeta(t, x_n)) \leq 0$
- $\xi, t \models \neg\phi$ iff not $\xi, t \models \phi$
- $\xi, t \models \phi \wedge \psi$ iff $\xi, t \models \phi$ and $\xi, t \models \psi$
- $\xi, t \models \phi \mathbb{U}_{\mathcal{J}} \psi$
  iff $\exists t' \in \mathcal{J} : \xi, max\{t' + t, 0\} \models \psi$ and $\forall t \leq t'' < t' + t : \xi, t'' \models \phi$

Additionally we define for a set of runs Ξ:

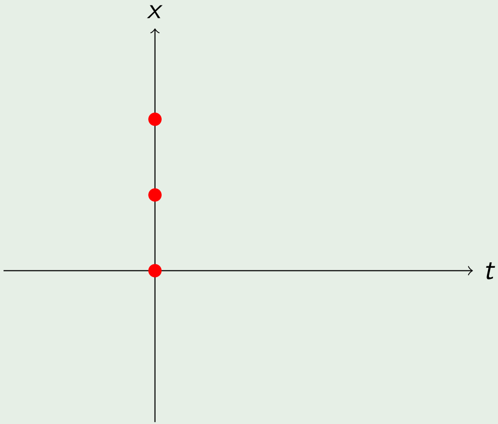
$$\Xi, t \models \phi \text{ iff for all runs } \xi \in \Xi \text{ holds } \xi, t \models \phi$$

A hybrid system H satisfies a formula denoted by $H \models \phi$ iff $\Xi_H, 0 \models \phi$.

Preservation (Informal)

Example

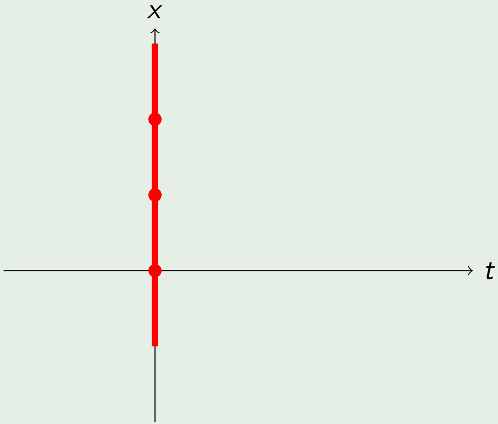
Formula: $x \in \{0, 1, 2\}$



Preservation (Informal)

Example

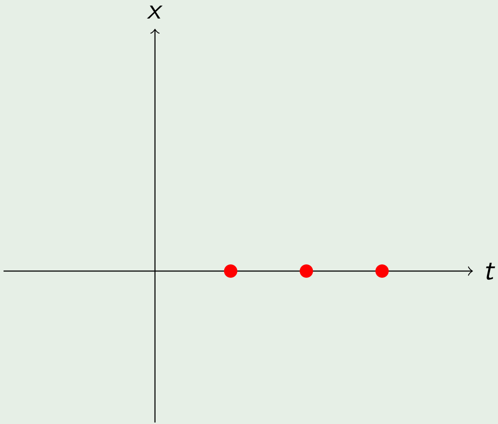
Formula: $x \in \{0, 1, 2\}$, $\delta = 1 \rightsquigarrow x \in [-1, 3]$



Preservation (Informal)

Example

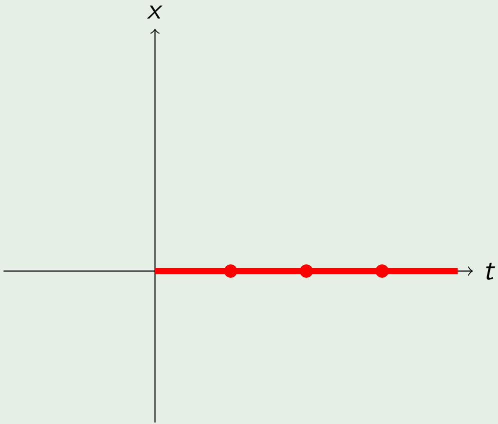
Formula: $\phi \mathbb{U}_{\{1,2,3\}} \psi$



Preservation (Informal)

Example

Formula: $\phi \mathbb{U}_{\{1,2,3\}} \psi$, $\varepsilon = 1 \rightsquigarrow \phi' \mathbb{U}_{[0,4]} \psi'$



Preservation (Formal)

Theorem (Preservation of logical properties)

If hybrid systems A and B satisfy $A \trianglelefteq^{\varepsilon,\delta} B$ and $B \models \phi$ then $A \models \phi^{+\delta}_{+\varepsilon}$ where $\phi^{+\delta}_{+\varepsilon} := re_{\varepsilon,\delta}(\phi)$ and $re_{\varepsilon,\delta}$ is defined by:

- $re_{\varepsilon,\delta}(x \in \mathcal{I}) := x \in \mathcal{I}'$, *where* $\mathcal{I}' = \{a \mid \exists b \in \mathcal{I} : a \in [b - \delta, b + \delta]\}$.
- $re_{\varepsilon,\delta}(f(x_1, \dots, x_n) \leq 0) := f(x_1, \dots, x_n) - \delta \cdot M \leq 0$ *where M is the Lipschitz constant for f.*

where $\mathcal{I} \subseteq \mathbb{R}$ and $\mathcal{J} \subseteq \mathbb{R}$ holds.

Preservation (Formal)

Theorem (Preservation of logical properties)

If hybrid systems A and B satisfy $A \trianglelefteq^{\varepsilon,\delta} B$ and $B \models \phi$ then $A \models \phi^{+\delta}_{+\varepsilon}$ where $\phi^{+\delta}_{+\varepsilon} := re_{\varepsilon,\delta}(\phi)$ and $re_{\varepsilon,\delta}$ is defined by:

- $re_{\varepsilon,\delta}(x \in \mathcal{I}) := x \in \mathcal{I}'$, *where* $\mathcal{I}' = \{a \mid \exists b \in \mathcal{I} : a \in [b-\delta, b+\delta]\}$.
- $re_{\varepsilon,\delta}(f(x_1,\ldots,x_n) \leq 0) := f(x_1,\ldots,x_n) - \delta \cdot M \leq 0$ *where M is the Lipschitz constant for f.*
- $re_{\varepsilon,\delta}(\neg\phi) := \neg ro_{\varepsilon,\delta}(\phi)$.
- $re_{\varepsilon,\delta}(\phi \wedge \psi) := re_{\varepsilon,\delta}(\phi) \wedge re_{\varepsilon,\delta}(\psi)$.

where $\mathcal{I} \subseteq \mathbb{R}$ and $\mathcal{J} \subseteq \mathbb{R}$ holds.

Preservation (Formal)

Theorem (Preservation of logical properties)

If hybrid systems A and B satisfy $A \trianglelefteq^{\varepsilon,\delta} B$ and $B \models \phi$ then $A \models \phi^{+\delta}_{+\varepsilon}$ where $\phi^{+\delta}_{+\varepsilon} := re_{\varepsilon,\delta}(\phi)$ and $re_{\varepsilon,\delta}$ is defined by:

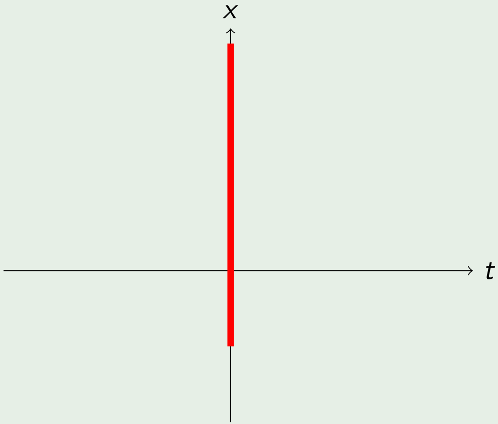
- $re_{\varepsilon,\delta}(x \in \mathcal{I}) := x \in \mathcal{I}'$, *where* $\mathcal{I}' = \{a \mid \exists b \in \mathcal{I} : a \in [b - \delta, b + \delta]\}$.
- $re_{\varepsilon,\delta}(f(x_1, \dots, x_n) \leq 0) := f(x_1, \dots, x_n) - \delta \cdot M \leq 0$ *where M is the Lipschitz constant for f.*
- $re_{\varepsilon,\delta}(\neg\phi) := \neg ro_{\varepsilon,\delta}(\phi)$.
- $re_{\varepsilon,\delta}(\phi \wedge \psi) := re_{\varepsilon,\delta}(\phi) \wedge re_{\varepsilon,\delta}(\psi)$.
- $re_{\varepsilon,\delta}(\phi \mathbb{U}_{\mathcal{J}} \psi) := re_{\varepsilon,\delta}(\phi) \mathbb{U}_{\mathcal{J}'} re_{\varepsilon,\delta}(\psi)$, *where* $\mathcal{J}' = \{a \mid \exists b \in \mathcal{J} : a \in [b - \varepsilon, b + \varepsilon]\}$.

where $\mathcal{I} \subseteq \mathbb{R}$ and $\mathcal{J} \subseteq \mathbb{R}$ holds.

Preservation (Informal)

Example

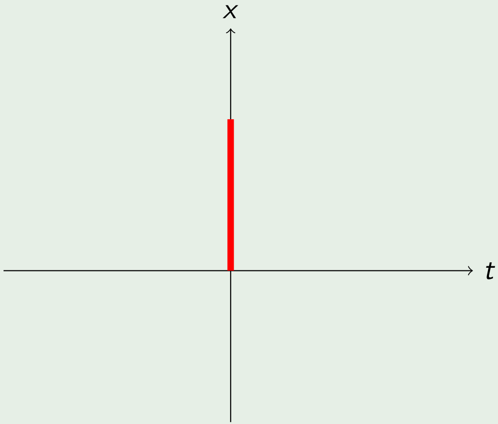
Formula: $\neg x \in [-1, 3]$



Preservation (Informal)

Example

Formula: $\neg x \in [-1, 3]$, $\delta = 1 \rightsquigarrow \neg x \in [0, 2]$



Preservation (Formal)

Theorem (Preservation of logical properties)

The transformation function $ro_{\varepsilon,\delta}$ *is given by:*

- $ro_{\varepsilon,\delta}(x \in \mathcal{I}) := x \in \mathcal{I}'$, *where* $\mathcal{I}' = \{a \mid \forall b \in [a-\delta, a+\delta] : b \in \mathcal{I}\}$.
- $ro_{\varepsilon,\delta}(f(x_1,\ldots,x_n) \le 0) := f(x_1,\ldots,x_n) + \delta \cdot M \le 0$ *where* M *is the Lipschitz constant for* f.

where $\mathcal{I} \subseteq \mathbb{R}$ *and* $\mathcal{J} \subseteq \mathbb{R}$ *holds.*

Preservation (Formal)

Theorem (Preservation of logical properties)

The transformation function $ro_{\varepsilon,\delta}$ is given by:

- $ro_{\varepsilon,\delta}(x \in \mathcal{I}) := x \in \mathcal{I}'$, *where* $\mathcal{I}' = \{a \mid \forall b \in [a-\delta, a+\delta] : b \in \mathcal{I}\}$.
- $ro_{\varepsilon,\delta}(f(x_1,\ldots,x_n) \le 0) := f(x_1,\ldots,x_n) + \delta \cdot M \le 0$ *where* M *is the Lipschitz constant for* f.
- $ro_{\varepsilon,\delta}(\neg\phi) := \neg re_{\varepsilon,\delta}(\phi)$.
- $ro_{\varepsilon,\delta}(\phi \wedge \psi) := ro_{\varepsilon,\delta}(\phi) \wedge ro_{\varepsilon,\delta}(\psi)$.

where $\mathcal{I} \subseteq \mathbb{R}$ *and* $\mathcal{J} \subseteq \mathbb{R}$ *holds.*

Preservation (Formal)

Theorem (Preservation of logical properties)

The transformation function $ro_{\varepsilon,\delta}$ is given by:

- $ro_{\varepsilon,\delta}(x \in \mathcal{I}) := x \in \mathcal{I}'$, *where* $\mathcal{I}' = \{a \mid \forall b \in [a-\delta, a+\delta] : b \in \mathcal{I}\}$.
- $ro_{\varepsilon,\delta}(f(x_1,\ldots,x_n) \leq 0) := f(x_1,\ldots,x_n) + \delta \cdot M \leq 0$ *where* M *is the Lipschitz constant for* f.
- $ro_{\varepsilon,\delta}(\neg\phi) := \neg re_{\varepsilon,\delta}(\phi)$.
- $ro_{\varepsilon,\delta}(\phi \wedge \psi) := ro_{\varepsilon,\delta}(\phi) \wedge ro_{\varepsilon,\delta}(\psi)$.
- $ro_{\varepsilon,\delta}(\phi \mathbb{U}_{\mathcal{J}} \psi) := ro_{\varepsilon,\delta}(\phi) \mathbb{U}_{\mathcal{J}'} ro_{\varepsilon,\delta}(\psi)$, *where* $\mathcal{J}' = \{a \mid \forall b \in [a-\varepsilon, a+\varepsilon] : b \in \mathcal{J}\}$.

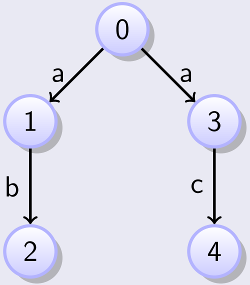
where $\mathcal{I} \subseteq \mathbb{R}$ *and* $\mathcal{J} \subseteq \mathbb{R}$ *holds.*

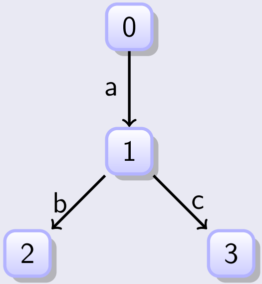
Outline

Classical Relation

Observation

Simulations can be defined in terms of games.





Observation

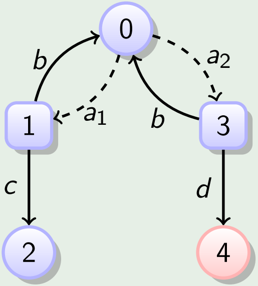
Controller synthesis is a game as well, i.e. the question whether the controller can win against an malicious environment.

Classical Relation

Observation

Controller synthesis is a game as well, i.e. the question whether the controller can win against an malicious environment.

Example



Hybrid Game

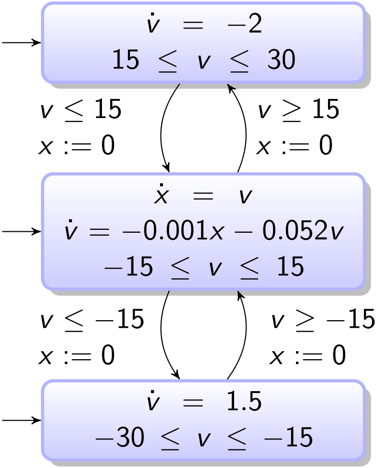
Definition (Hybrid Game)

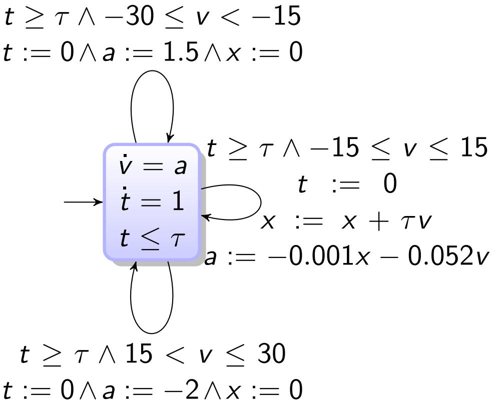
A *hybrid game* $HG = (S, E_c, U_c, l)$ consists of

- a hybrid automaton $S = (U, X, L, E, F, Inv, Init)$,
- a set of controllable transitions $E_c \subseteq E$,
- a set of controllable variables $U_c \subseteq U$,
- and a location $l \in L$.

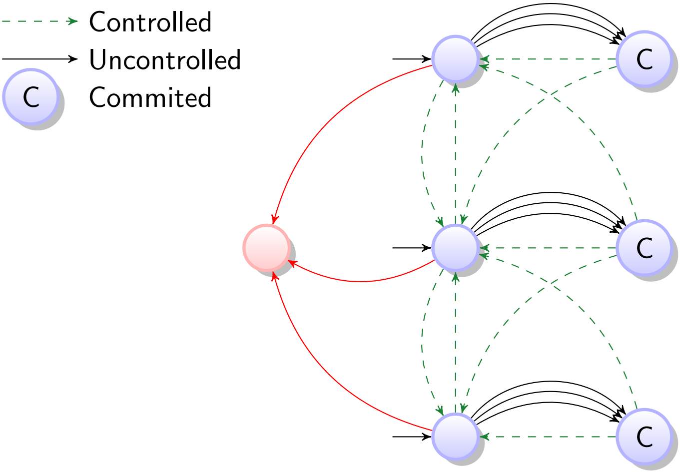
The environment wins, if it can force the game to enter the location l or if the controller does not have any more moves. The controller wins, if he can assert that the location l is avoided.

Velocity Controller





Velocity Controller (Game)



$U_c = \{s\}$ Invariant: $0 \leq s \leq 2$

$\dot{v} = -0.001x - 0.052v \rightsquigarrow \dot{v} = s \cdot (-0.001x - 0.052v)$

$\dot{v} = a \rightsquigarrow \dot{v} = (2 - s) \cdot a$

Similarity and Games

Assumption

The systems that we compare are inputless, i.e. $U = \emptyset$.

Theorem

Given two hybrid systems A and B. If there is a winning strategy for the controller in the game $(A \lessdot B, E_c, \{s\}, bad)$ *then* $A \trianglelefteq^{\varepsilon,\delta} B$ *holds.*

Observation

If system B is deterministic and a retiming strategy is given, model checking can be used to show that the winning strategy exists.

Outline

Summary

We . . .

- . . . defined a notion of similarity for hybrid systems.
- . . . showed properties that are preserved by this notion.
- . . . established the classical relation between simulations and games for this notion.
- . . . established some preliminary results for solving these games.